# Internet Filtering: CIPA Compliance

Lauren Abner

Kentucky Department for Libraries and Archives

502-564-1728

lauren.abner@ky.gov

# Children's Internet Protection Act

- "The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress [in 2000] to address concerns about access to offensive content over the Internet on school and library computers."

www.fcc.gov/guides/childrens-internet-protection-act

# Does my library have to comply?

- Libraries must comply with CIPA if they receive certain federal funding:
  - E-rate – libraries applying for discounts on Internet Access (Category One) or eligible equipment (Category Two)
    - Exempt: libraries applying only for telecommunications service
  - LSTA – libraries applying for computers or internet access with these funds

# Children’s Internet Protection Act


Technology Protection Measure

Internet Safety Policy

Notice & Public Meeting

# General Resources

- https://transition.fcc.gov/cgb/consumerfacts/cipa.pdf
  - The basics from the FCC.
- http://www.e-ratecentral.com/CIPA/cipa_checklist.pdf
  - E-rate Central's brief checklist for CIPA compliance.
- http://www.ala.org/advocacy/advleg/federallegislation/cipa/
  - FAQ and legal history
- http://www.webjunction.org/documents/webjunction/CIPA_Key_Issues_for_Decision_Makers.html
  - Legal definitions and resources list

# In general, how do content filters work?

- Filtering can be accomplished by installing software on individual computers, adding hardware to a local area network (LAN), or using a cloud-based filter
- Content filters usually involve several methods for blocking undesired content, including:
  - Blocking certain URLs or entire domains
  - Dynamic content filtering based on keywords or phrases, ad placement, and link analysis
  - Blocking certain file types (audio, image, or executable files)
  - Limiting or blocking bandwidth for certain sites – many schools do this for social media and music streaming
  - In combination with security or firewall features, blocking viruses and malware
- Can work with service provider to change settings, 'whitelist' sites

# What the TPM must block

- This technology must block or filter Internet access to **visual depictions** that are classified as:
  - Obscene
  - Child Pornography
  - Harmful to minors (this requirement applies to those under the age of 17 only)
- Does not apply to text or audio

# Legal Requirements of CIPA

- Obscenity
  - 18 U.S.C. § 1460
  - Miller Obscenity Test (AKA '3 prong standard')– "average person applying contemporary community standards" must find that the image:
    - appeals to the prurient interest;
    - is patently offensive; and
    - has no literary, scientific, artistic, or political value whatsoever.
- Child Pornography
  - 18 U.S.C. § 2256
  - Any visual depiction (including computer-generated) that appears to be a minor engaging in sexual conduct.
- Harmful to Minors (under 17)
  - 18 U.S.C. § 2246
  - Legally, only sexual material is harmful to minors.
  - Does not include graphic violence, hate speech, drug use, etc.

# More on legal definitions

- Access to child pornography, obscenity, and material harmful to minors (by minors, does not apply to adults) has never been protected by the First Amendment.
  - **No one has the right to view child pornography or obscene material in your library.**
- The legal definitions of these terms are **very narrow** and rarely correspond to the categories used by companies providing content filtering.
  - Most filters will undoubtedly block more content than is required by CIPA.

# Common misconceptions about CIPA

CIPA does not require:

- Monitoring or tracking of individual patrons.
- Any library or other agency to certify the effectiveness of filtering software.
- A specific set of procedures to unblock the filter.
- Filtering of categories other than child pornography, obscenity, and material harmful to minors.
- Blocking social media sites like YouTube or Facebook

# Implementing a Filter

- All Internet access on computers (desktops & laptops) owned by the library must be filtered.
  - This includes staff computers that may not ordinarily be visible to minors.
  - Some libraries employ staff and volunteers younger than 17.
- CIPA does not require filtering of patron-owned laptops, only of library-owned computers.
  - However, if library-owned laptops use the library's wifi, wireless access must be filtered.

# Disabling the Filter

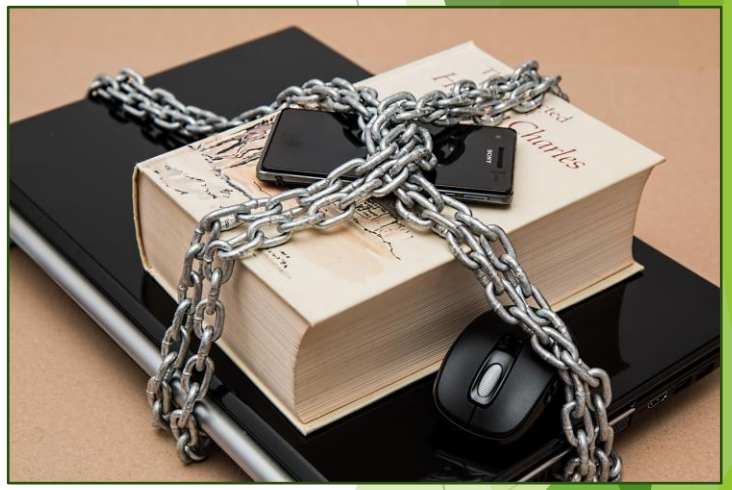
- The filter can be lifted or sites unblocked for anyone 17 or older.
  - The original language (2000) specifies that the library may disable the protection measure for “research or other lawful purposes”.
  - During arguments before the Supreme Court in 2003, the Solicitor General confirmed that a patron would not have to state why they asked for a site to be unblocked.
- Allowing the filter to be disabled was a **critical** element in CIPA’s not being declared unconstitutional by the Supreme Court in 2003.
  - Failing to lift the filter or unblock sites could open your library to “as-applied” legal challenges

# Best Practices for Filtering

- Allow easy unblocking of websites and/or lifting of the filter.
- Block only what is required by CIPA or what your community determines at the public meeting.
- Refine your filter configuration.
  - Some libraries have online forms to report access issues: http://denverlibrary.org/content/request-reconsideration-access-web-site
- Personalize the block screen.
  - Let patrons know why they have been denied access to a particular site, and how to go about getting the website unblocked.

# The Limits of Filtering

- The law does not mandate that the filter work perfectly.
  - Libraries must make a good faith effort to remove visual depictions of obscenity, child pornography, and material harmful to minors from library computers.
  - No person or agency can guarantee the effectiveness of any filter.
- Decisions about which filter to implement, unblocking procedures, and whether or not to filter wireless access are made at the local level.



# Filtering resources

- http://libraryfiltering.org/
  - One of the few unbiased filtering review sites on the web.
- http://community.spiceworks.com/spice_lists/94
  - IT community's ranked list of content filtering software
- http://www.webjunction.org/documents/webjunction/Understanding_Content_Filtering_An_FAQ_for_Nonprofits.html/
  - A great introduction to how filters work and best practices.
- http://www.ala.org/advocacy/intfreedom/filtering
  - ALA's Filters and Filtering page arguing in favor of intellectual freedom

# Internet Safety Policy

## 5 required elements

1. Access by minors to inappropriate matter on the Internet;
2. Safety and security of minors when using email, chat rooms, and other forms of direct electronic communications;
3. Unauthorized access, including hacking, and other unlawful activities by minors online;
4. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and
5. Measures designed to restrict minors' access to materials that may be harmful to minors.

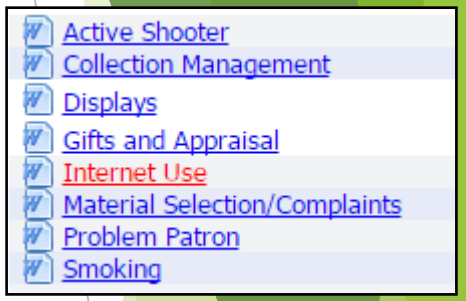
***Bonus*** The Technology Protection Measure (filter) should also be incorporated.

# Policy Best Practices

- Wording
  - Avoid First Amendment legal challenges by sticking closely to what is required by CIPA.
  - For example, the word “obscene” has a legal definition, while the word “explicit” does not.
- Consult a lawyer, if possible!
  - If not, model your policy on a pre-existing one.

# Sample Internet Policies

- kdla.ky.gov/librarians/librarypolicies/Pages/LibraryOperationsPolicies.aspx There are examples of several Internet use policies brought together in one document on KDLA's website. Sample #2 includes the 5 required elements.
- e-ratecentral.com/CIPA/cipa_policy_sample.pdf E-rate Central's guide includes a basic sample policy.



# Public meeting

- "A library…shall provide **reasonable public notice** and hold at least one public hearing or meeting to address the proposed Internet safety policy."
  - 47 U.S.C. § 254 (h)(6)(A)(iii)
- The meeting must follow the guidelines of the Kentucky Open Meetings Act.
  - KRS 61.823
- The notice to the public must also comply with state law.
  - KRS 424.130 (1)(d), KRS 424.120

# Public meeting, continued

- This meeting may be held as part of a regular library board meeting as long as:
  - the agenda is advertised; and
  - the opportunity for public comment is allowed.
- This is an opportunity to explain why these policies are being adopted and how they will benefit taxpayers.

# Compliance – E-rate Timeline

- 1st Year of compliance
  - 1st year after FY2001 that the library applied for services other than telecommunications **AND** filed a Form 486.
  - Check the E-rate Central website to determine when a Form 486 was last filed for your library (enter your BEN):

    http://www.e-ratecentral.com/us/stateInformation.asp?state=KY
  - Must document that you are moving toward compliance. For more information about acceptable documentation, see the SLD website: http://www.usac.org/sl/applicants/step06/cipa.aspx
- 2nd Year and subsequent years
  - Must be compliant if applying for E-rate again.

# Documentation of Compliance

- Copy of Internet Safety Policy
- Technology Protection Measure (filter)
  - Maintenance logs, filtering logs, proof of purchase, procurement paperwork, etc.
- Proof of public meeting
  - May be held as part of a regular board meeting as long as public comments are allowed.
- Proof of notice of public meeting
  - Meeting must be advertised in advance.
- Documentation must be retained for 10 years for E-rate.
  - See USAC website for more information: http://www.usac.org/sl/applicants/step06/cipa.aspx


# Questions?

## Lauren Abner

Technology Consultant

Kentucky Department for Libraries & Archives

lauren.abner@ky.gov

502-564-1728